日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　６月２６日

出願番号
Application Number: 特願２００３－１８２２２２

[ST. 10/C]: [ＪＰ２００３－１８２２２２]

出願人
Applicant(s): コニカミノルタビジネステクノロジーズ株式会社

２００４年　２月　４日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３００５８９５

【書類名】　特許願
【整理番号】　DTS00039
【あて先】　特許庁長官殿
【国際特許分類】　H04N　1/44
【発明者】
　【住所又は居所】　東京都八王子市石川町２９７０番地　コニカビジネステクノロジーズ株式会社内
　【氏名】　小田　昭彦
【特許出願人】
　【識別番号】　303000372
　【氏名又は名称】　コニカビジネステクノロジーズ株式会社
【代理人】
　【識別番号】　100121599
　【弁理士】
　【氏名又は名称】　長石　富夫
【手数料の表示】
　【予納台帳番号】　203058
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0305288
【プルーフの要否】　要

【書類名】明細書

【発明の名称】　データ秘密化装置、データ復元装置、画像データ保存装置及び画像形成装置

【特許請求の範囲】

【請求項１】

圧縮後のデータの一部でも正しくないと伸張処理ができない圧縮方式でデータを圧縮して得た圧縮データの一部を暗号キーデータとして取り出す暗号キー抽出手段と、

圧縮データのうち暗号キーデータとして取り出された部分を前記暗号キーデータと異なるデータで置き換えることで前記圧縮データを暗号化する暗号化手段と、

を有する

ことを特徴とするデータ秘密化装置。

【請求項２】

圧縮後のデータの一部でも正しくないと伸張処理ができない圧縮方式でデータを圧縮して得た圧縮データの一部を暗号キーデータとして取り出す暗号キー抽出手段と、

圧縮データのうち暗号キーデータとして取り出された部分を削除することで前記圧縮データを暗号化する暗号化手段と、

を有する

ことを特徴とするデータ秘密化装置。

【請求項３】

圧縮データの先頭から所定範囲を前記暗号キーデータにする

ことを特徴とする請求項１または２に記載のデータ秘密化装置。

【請求項４】

請求項１または２に記載のデータ秘密化装置によって同一の圧縮データから生成された暗号キーデータと暗号化後の圧縮データとを組み合わせて、暗号化される前の圧縮データを復元する圧縮データ復元手段

を有する

ことを特徴とするデータ復元装置。

【請求項５】

圧縮後のデータの一部でも正しくないと伸張処理ができない圧縮方式でデータを圧縮する圧縮手段と、

前記圧縮手段によって画像データを圧縮して得た圧縮データの一部を暗号キーデータとして取り出す暗号キー抽出手段と、

圧縮データのうち暗号キーデータとして取り出された部分を前記暗号キーデータと異なるデータで置き換えて前記圧縮データを暗号化する暗号化手段と、

前記暗号キー抽出手段が取り出した暗号キーデータを保存する暗号キー保存手段と、

前記暗号化手段によって圧縮データを暗号化して得た暗号化データを保存する暗号化データ保存手段と、

同一の圧縮データから得た暗号キーデータと暗号化データとの対応付けを表した管理情報を記憶する管理情報記憶手段と、

前記管理情報記憶手段に記憶されている管理情報に基づいて、同一の圧縮データから得た暗号キーデータと暗号化データとを前記暗号キー保存手段と前記暗号化データ保存手段から取り出し、これらを組み合わせて元の圧縮データに復元する圧縮データ復元手段と、

前記圧縮データ復元手段によって復元された圧縮データを圧縮前の画像データに伸張する伸張手段と

を有する

ことを特徴とする画像データ保存装置。

【請求項６】

圧縮後のデータの一部でも正しくないと伸張処理ができない圧縮方式でデータを圧縮する圧縮手段と、

前記圧縮手段によって画像データを圧縮して得た圧縮データの一部を暗号キーデータとして取り出す暗号キー抽出手段と、

圧縮データのうち暗号キーデータとして取り出された部分を削除して前記圧縮データを暗号化する暗号化手段と、

前記暗号キー抽出手段が取り出した暗号キーデータを保存する暗号キー保存手段と、

前記暗号化手段によって圧縮データを暗号化して得た暗号化データを保存する暗号化データ保存手段と、

同一の圧縮データから得た暗号キーデータと暗号化データとの対応付けを表した管理情報を記憶する管理情報記憶手段と、

前記管理情報記憶手段に記憶されている管理情報に基づいて、同一の圧縮データから得た暗号キーデータと暗号化データとを前記暗号キー保存手段と前記暗号化データ保存手段から取り出し、これらを組み合わせて元の圧縮データに復元する圧縮データ復元手段と、

前記圧縮データ復元手段によって復元された圧縮データを圧縮前の画像データに伸張する伸張手段と

を有する

ことを特徴とする画像データ保存装置。

【請求項７】

圧縮後のデータの一部でも正しくないと伸張処理ができない圧縮方式で画像データを圧縮する圧縮手段と、

前記圧縮手段によって画像データを圧縮して得た圧縮データの一部を暗号キーデータとして取り出す暗号キー抽出手段と、

圧縮データのうち暗号キーデータとして取り出された部分を前記暗号キーデータと異なるデータに置き換えて前記圧縮データを暗号化する暗号化手段と、

前記暗号化手段によって圧縮データを暗号化して得た暗号化データを保存する暗号化データ保存手段と、

前記暗号キー抽出手段が抽出した暗号キーデータと、この暗号キーデータに対応する暗号化データを特定するための特定情報とを関連付けて外部のユーザーに所定の形態で出力する復元情報出力手段と

を有する

ことを特徴とする画像データ保存装置。

【請求項８】

圧縮後のデータの一部でも正しくないと伸張処理ができない圧縮方式で画像データを圧縮する圧縮手段と、

前記圧縮手段によって画像データを圧縮して得た圧縮データの一部を暗号キーデータとして取り出す暗号キー抽出手段と、

圧縮データのうち暗号キーデータとして取り出された部分を削除して前記圧縮データを暗号化する暗号化手段と、

前記暗号化手段によって圧縮データを暗号化して得た暗号化データを保存する暗号化データ保存手段と、

前記暗号キー抽出手段が抽出した暗号キーデータとこの暗号キーデータに対応する暗号化データを特定するための特定情報とを関連付けて外部のユーザーに所定の形態で出力する復元情報出力手段と

を有する

ことを特徴とする画像データ保存装置。

【請求項９】

暗号キーデータとこれに関連付けされた特定情報とを入力する復元情報入力手段と、

前記復元情報入力手段を通じて入力された特定情報に対応する暗号化データを前記暗号化データ保存手段から取り出し、これと前記入力された暗号キーデータとを組み合わせて暗号化される前の圧縮データを復元する圧縮データ復元手段と、

前記圧縮データ復元手段によって復元された圧縮データを圧縮前の画像データに伸張する伸張手段と

をさらに有する

ことを特徴とする請求項７または８に記載の画像データ保存装置。

【請求項１０】

圧縮データの先頭から所定範囲を前記暗号キーデータにする

ことを特徴とする請求項５、６、７、８または９に記載の画像データ保存装置。

【請求項１１】

原稿を読み取って対応する画像データを取り込む読取手段と、

前記読取手段が取り込んだ画像データを圧縮し暗号化して保存する請求項５から請求項１０のいずれかに記載の画像データ保存装置と、

画像データに対応する画像を記録紙上に形成して出力する印刷手段と

を有する

ことを特徴とする画像形成装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データを暗号化するデータ秘密化装置、暗号化されたデータを復元するデータ復元装置、画像データを圧縮して保存する機能を備えた画像データ保存装置およびこれを用いた画像形成装置に関する。

【０００２】

【従来の技術】

近年、コピー機能を備えた複写機やこれにスキャナー機能、プリンタ機能、ファクシミリ機能などを付加したデジタル複合機などの画像形成装置では、読み取った原稿画像を電子データ（画像データ）として、メモリやハードディスク装置（ＨＤＤ）などの記憶媒体に記憶する機能を有している。この機能を利用して、記憶媒体に記憶された画像データを、ユーザーの指示に基づいて、通信回線を通じて外部の装置に送信したり、後で再プリントしたりすることが可能になっている。

【０００３】

しかしその一方、画像データが電子データとして画像形成装置本体に保存されているため、保存されている機密文書を第三者に勝手に印刷して持ち去られたり、機密データが電子メールで外部に送信されたり、ネットワークを介して外部に取り出されたりするなどの脅威が発生する。そのため、画像形成装置にセキュリティ機能が求められるようになり、たとえば、本体に保存された文書を取り出す際にパスワードによる認証を求めたり、文書データや画像データを暗号化して保存したりするなどの技術が普及し始めている（たとえば、特許文献１参照。）。

【０００４】

【特許文献１】

特許第３３７５６３１号公報

【０００５】

【発明が解決しようとする課題】

文書データや画像データを暗号化して保存する技術はセキュリティーの向上にとって有効性が高く、様々な暗号化方式が実用化されている。しかしながら複写機やデジタル複合機などで扱われる画像データは、非常に情報量が多いので、その暗号化処理や復号化処理の実行に長い時間を要してしまう。このため、画像データを暗号化することによってセキュリティ性を高める方法を採用すると、暗号化処理や復号化処理がＣＰＵを独占する時間が増え、画像形成装置自体としての生産性が低下してしまうという問題が発生する。

【０００６】

そこで、暗号化や復号化のための専用チップを搭載してＣＰＵの負担を軽減することも行なわれるが、この方法を用いて既存の機種にセキュリティ機能を追加するためにはハードウェアの改造が必要で製品の価格が高騰してしまうという問題がある。

【０００７】

本発明は、このような従来の技術が有する問題点に着目してなされたもので、特別なハードウェアの追加やＣＰＵに大きな負担をかけることなく、画像データ等のデータを高速に暗号化・復号化することのできるデータ秘密化装置、データ復元装置、画像データ保存装置及び画像形成装置を提供することを目的としている。

【０００８】

【課題を解決するための手段】

かかる目的を達成するための本発明の要旨とするところは、次の各項の発明に存する。

請求項１にかかわる発明は、圧縮後のデータの一部でも正しくないと伸張処理ができない圧縮方式でデータを圧縮して得た圧縮データの一部を暗号キーデータ

として取り出す暗号キー抽出手段（２０１）と、圧縮データのうち暗号キーデータとして取り出された部分を前記暗号キーデータと異なるデータで置き換えることで前記圧縮データを暗号化する暗号化手段（２０２）と、を有することを特徴とするデータ秘密化装置である。

【０００９】

上記発明によれば、圧縮データの一部でも正しくないと伸張処理ができない圧縮方式でデータを圧縮して得た圧縮データの一部を取り出して暗号キーデータとする一方、圧縮データのうち暗号キーデータとして取り出した部分を破壊することで圧縮データを暗号化している。圧縮データの一部でも正しくないと伸張処理ができない圧縮方式としては、たとえばＬＺ圧縮方式がある。特に、本発明による暗号化には、前方のデータ（辞書）を参照しながら後方のデータを復号化する圧縮方式が好適である。

【００１０】

暗号化は、圧縮データのうち暗号キーデータが取り出された部分を暗号キーデータと異なる値に置き換えることで可能であるが、より確実に復元不能とするためには、その部分をゼロクリアするとよい。つまり、暗号キーデータと相関が無く充分に相違するデータで置き換えることが望ましい。また暗号キーデータとして取り出すデータ量が多いほど、セキュリティレベルは高まる。暗号キーデータを、圧縮データの複数箇所から抽出したり、抽出する箇所自体にも暗号性を持たせたりするとさらによい。

【００１１】

このように、簡単な処理で圧縮データを暗号化できるので、特別なハードウェアの追加やＣＰＵに大きな負担をかけることなくデータを秘密化してセキュリティを高めることができる。特に、大量のデータを保存する際には、使用メモリ量を少なくするために圧縮処理が施されるが、本発明では、圧縮後の圧縮データの性質を利用して暗号化するので、圧縮と暗号化とが効率よく実現される。

【００１２】

請求項２にかかわる発明は、圧縮後のデータの一部でも正しくないと伸張処理ができない圧縮方式でデータを圧縮して得た圧縮データの一部を暗号キーデータ

として取り出す暗号キー抽出手段（２０１）と、圧縮データのうち暗号キーデータとして取り出された部分を削除することで前記圧縮データを暗号化する暗号化手段（２０２）と、を有することを特徴とするデータ秘密化装置である。

【００１３】

上記発明によれば、圧縮データの一部でも正しくないと伸張処理ができない圧縮方式でデータを圧縮して得た圧縮データの一部を取り出して暗号キーデータとし、暗号キーデータとして取り出した部分を削除することで圧縮データが暗号化される。たとえば、圧縮データを暗号キーデータ（１５１）の部分とそれ以外の部分（１５２）に分割することで、暗号キーデータの取り出しと該当部分の削除が可能になる。

【００１４】

請求項３にかかわる発明は、圧縮データの先頭から所定範囲を前記暗号キーデータにすることを特徴とする請求項１または２に記載のデータ秘密化装置である。

【００１５】

圧縮データの一部でも正しくないと伸張処理ができない圧縮方式では、圧縮データの先頭部分が伸張のために重要な役割を果たしていることが多いので、この先頭部分を破壊したり削除したりすることで、最初から一切の伸張を阻止することができ、セキュリティ性を高めることができる。

【００１６】

請求項４にかかわる発明は、請求項１または２に記載のデータ秘密化装置によって同一の圧縮データから生成された暗号キーデータと暗号化後の圧縮データとを組み合わせて、暗号化される前の圧縮データを復元する圧縮データ復元手段（２２１）を有することを特徴とするデータ復元装置である。

【００１７】

上記発明によれば、暗号化された圧縮データのうち破壊や削除されている部分が暗号キーデータによって修復され、伸張が可能になる。暗号化された圧縮データをこのように簡単な処理により伸張可能な圧縮データに復元することができるので、特別なハードウェアの追加やＣＰＵに大きな負担をかけることなく、高速

な復元が実現される。

【００１８】

請求項５にかかわる発明は、圧縮後のデータの一部でも正しくないと伸張処理ができない圧縮方式でデータを圧縮する圧縮手段（２８）と、前記圧縮手段（２８）によって画像データを圧縮して得た圧縮データの一部を暗号キーデータとして取り出す暗号キー抽出手段（３１）と、圧縮データのうち暗号キーデータとして取り出された部分を前記暗号キーデータと異なるデータで置き換えて前記圧縮データを暗号化する暗号化手段（３２）と、前記暗号キー抽出手段（３１）が取り出した暗号キーデータを保存する暗号キー保存手段（５１）と、前記暗号化手段（３２）によって圧縮データを暗号化して得た暗号化データを保存する暗号化データ保存手段（４０）と、同一の圧縮データから得た暗号キーデータと暗号化データとの対応付けを表した管理情報を記憶する管理情報記憶手段（５２）と、前記管理情報記憶手段（５２）に記憶されている管理情報に基づいて、同一の圧縮データから得た暗号キーデータと暗号化データとを前記暗号キー保存手段（５１）と前記暗号化データ保存手段（４０）から取り出し、これらを組み合わせて元の圧縮データに復元する圧縮データ復元手段（３３）と、前記圧縮データ復元手段（３３）によって復元された圧縮データを圧縮前の画像データに伸張する伸張手段（２９）とを有することを特徴とする画像データ保存装置である。

【００１９】

請求項６にかかわる発明は、圧縮後のデータの一部でも正しくないと伸張処理ができない圧縮方式でデータを圧縮する圧縮手段（２８）と、前記圧縮手段（２８）によって画像データを圧縮して得た圧縮データの一部を暗号キーデータとして取り出す暗号キー抽出手段（３１）と、圧縮データのうち暗号キーデータとして取り出された部分を削除して前記圧縮データを暗号化する暗号化手段（３２）と、前記暗号キー抽出手段（３１）が取り出した暗号キーデータを保存する暗号キー保存手段（５１）と、前記暗号化手段（３２）によって圧縮データを暗号化して得た暗号化データを保存する暗号化データ保存手段（４０）と、同一の圧縮データから得た暗号キーデータと暗号化データとの対応付けを表した管理情報を記憶する管理情報記憶手段（５２）と、前記管理情報記憶手段（５２）に記憶さ

れている管理情報に基づいて、同一の圧縮データから得た暗号キーデータと暗号化データとを前記暗号キー保存手段（５１）と前記暗号化データ保存手段（４０）から取り出し、これらを組み合わせて元の圧縮データに復元する圧縮データ復元手段（３３）と、前記圧縮データ復元手段（３３）によって復元された圧縮データを圧縮前の画像データに伸張する伸張手段（２９）とを有することを特徴とする画像データ保存装置である。

【００２０】

請求項５および請求項６に記載の発明によれば、圧縮データから取り出した暗号キーデータを暗号キー保存手段（５１）に保存し、圧縮データのうち暗号キーデータの部分を破壊や削除して得た暗号化データを暗号化データ保存手段（４０）に保存し、同一の圧縮データから得た暗号キーデータと暗号化データとの対応付けを表した管理情報を管理情報記憶手段（５２）に記憶する。これらにより、画像データが秘密化されて保存される。また画像データを伸張する際には、管理情報に基づいて暗号キー保存手段（５１）と暗号化データ保存手段（４０）とから対応する暗号キーデータと暗号化データとを取り出し、これらを組み合わせて元の圧縮データに復元した後、伸張される。したがって、ユーザーは装置内部で暗号化されていることを意識することなく画像データの保存と取り出しを行なうことができる。

【００２１】

また画像データを保存する場合は使用メモリ量を少なくするために圧縮処理を施すが、この圧縮処理で生成された圧縮データの性質を利用して暗号化するので、圧縮と暗号化とが効率的に実現される。

【００２２】

請求項７にかかわる発明は、圧縮後のデータの一部でも正しくないと伸張処理ができない圧縮方式で画像データを圧縮する圧縮手段（２８）と、前記圧縮手段（２８）によって画像データを圧縮して得た圧縮データの一部を暗号キーデータとして取り出す暗号キー抽出手段（３１）と、圧縮データのうち暗号キーデータとして取り出された部分を前記暗号キーデータと異なるデータに置き換えて前記圧縮データを暗号化する暗号化手段（３２）と、前記暗号化手段（３２）によっ

て圧縮データを暗号化して得た暗号化データを保存する暗号化データ保存手段（４０）と、前記暗号キー抽出手段（３１）が抽出した暗号キーデータとこの暗号キーデータに対応する暗号化データを特定するための特定情報とを関連付けて外部のユーザーに所定の形態で出力する復元情報出力手段（３４）とを有することを特徴とする画像データ保存装置である。

【００２３】

請求項８にかかわる発明は、圧縮後のデータの一部でも正しくないと伸張処理ができない圧縮方式で画像データを圧縮する圧縮手段（２８）と、前記圧縮手段（２８）によって画像データを圧縮して得た圧縮データの一部を暗号キーデータとして取り出す暗号キー抽出手段（３１）と、圧縮データのうち暗号キーデータとして取り出された部分を削除して前記圧縮データを暗号化する暗号化手段（３２）と、前記暗号化手段（３２）によって圧縮データを暗号化して得た暗号化データを保存する暗号化データ保存手段（４０）と、前記暗号キー抽出手段（３１）が抽出した暗号キーデータとこの暗号キーデータに対応する暗号化データを特定するための特定情報とを関連付けて外部のユーザーに所定の形態で出力する復元情報出力手段（３４）とを有することを特徴とする画像データ保存装置である。

【００２４】

請求項７および請求項８に記載の発明によれば、暗号化手段（３２）によって圧縮データを暗号化して得た暗号化データを装置内部の暗号化データ保存手段（４０）に保存する。一方、暗号キーデータとこの暗号キーデータに対応する暗号化データを特定するための特定情報とを関連付けて外部のユーザーに所定の形態で出力する。これにより暗号キーデータと特定情報を有するユーザーだけが画像データ保存装置に保存されている暗号化データを復元して伸張することが可能になる。ユーザーへの出力形態としては、記録紙への印刷出力や電子メール等による送信がある。特にユーザーに向けて出力した後で暗号キーデータや特定情報を画像データ保存装置から削除すれば、画像データ保存装置に残っている情報だけでは一切の復元ができなくなり、セキュリティ性がさらに高まる。

【００２５】

請求項９にかかわる発明は、暗号キーデータとこれに関連付けされた特定情報とを入力する復元情報入力手段（３５）と、前記復元情報入力手段（３５）を通じて入力された特定情報に対応する暗号化データを前記暗号化データ保存手段（４０）から取り出し、これと前記入力された暗号キーデータとを組み合わせて暗号化される前の圧縮データを復元する圧縮データ復元手段（３３）と、前記圧縮データ復元手段（３３）によって復元された圧縮データを圧縮前の画像データに伸張する伸張手段（２９）とをさらに有することを特徴とする請求項７または８に記載の画像データ保存装置である。

【００２６】

上記発明では、暗号キーデータと特定情報とを入力することで、保存されている暗号化データを画像データ保存装置自身で元の圧縮データに復元して伸張することができる。

【００２７】

請求項１０にかかわる発明は、圧縮データの先頭から所定範囲を前記暗号キーデータにすることを特徴とする請求項５、６、７、８または９に記載の画像データ保存装置である。

【００２８】

上記発明によれば、圧縮データの一部でも正しくないと伸張処理ができない圧縮方式では、圧縮データの先頭部分が伸張のために重要な役割を果たしていることが多いので、この先頭部分を破壊したり削除したりすることで、最初から一切の伸張を阻止することができ、セキュリティ性を高めることができる。

【００２９】

請求項１１にかかわる発明は、原稿を読み取って対応する画像データを取り込む読取手段（２３）と、前記読取手段（２３）が取り込んだ画像データを圧縮し暗号化して保存する請求項５から請求項１０のいずれかに記載の画像データ保存装置と、画像データに対応する画像を記録紙上に形成して出力する印刷手段（２４）とを有することを特徴とする画像形成装置である。

【００３０】

上記発明によれば、画像形成装置に保存された画像データを不正な第三者によ

る持ち出し閲覧から保護することができる。

【００３１】

【発明の実施の形態】

以下、図面に基づき本発明の各種実施の形態を説明する。

図１は、本発明の原理を示している。図中の実線矢印は圧縮・暗号化時のデータの流れを、破線矢印は復号化・伸張時のデータの流れを示している。本発明では、画像データ１０を圧縮し、圧縮後の圧縮データ１１の一部を取り出して暗号キーデータ１２にしている。図１の例では、圧縮データ１１の先頭から所定範囲の部分１１ａを暗号キーデータ１２として取り出している。一方、圧縮データ１１は、暗号キーデータ１２が取り出された部分１１ａをゼロクリアなどによって元の値と異なるデータに置き換えることで暗号化されて、暗号化データ１３に変換される。

【００３２】

圧縮データ１１への復元は、暗号化データ１３のうちゼロクリア等により破壊された部分１１ａに暗号キーデータ１２を戻すことで行なわれる。そして、復元された圧縮データを伸張することで圧縮前の画像データ１０が再生される。

【００３３】

画像データ１０の圧縮は、圧縮データの一部でも正しくないと伸張処理ができない圧縮方式で行なわれる。たとえば、ＬＺ圧縮などを用いる。ＬＺ圧縮は、圧縮すべきデータが以前に出現していなければ、そのデータを辞書として登録し、既に出現している場合は、同一のデータが登録されている辞書の位置と長さを記憶することによりデータを圧縮するようになっている。このような圧縮方式で圧縮された圧縮データの伸張には、前方のデータと比較することが必要になるので、前方のデータや辞書が壊れている場合には、元のデータに伸張することができなくなる。

【００３４】

圧縮方式は、上述したＬＺ圧縮に限らず、伸張処理において前方のデータの参照を必要とする他の方式や圧縮データの一部でも正しくないと伸張できない方式であれば如何なる方式であってもよい。

【００３５】

図２は、本発明の第１の実施の形態にかかわる画像データ保存装置を含む画像形成装置２０の構成を示している。画像形成装置２０は、原稿を読み取って対応する画像を記録紙上に形成して出力するコピー機能の他にスキャナー機能、プリンタ機能、ファクシミリ機能などを備えたデジタル複合機として構成されている。また、原稿を読み取って得た画像データを圧縮し暗号化して、あるいは暗号化せずに自装置内に保存する機能、圧縮し暗号化した画像データを電子メールやＦＴＰ（ファイル・トランスファ・プロトコル）を用いて外部の装置に送信する機能、保存されている画像を呼び出してプリントする機能などを備えている。

【００３６】

このような機能を実現すべく画像形成装置２０は、図２に示すように、画像データ制御部として機能するＣＰＵ（中央処理装置）３０と、ＲＯＭ（リード・オンリ・メモリ）２１とＲＡＭ（ランダム・アクセス・メモリ）２２とを主要部とした回路で構成されている。ＣＰＵ３０は、画像形成装置２０の動作を統括制御する。ＲＯＭ２１は、ＣＰＵ３０が実行するプログラムや各種固定データを記憶している。ＲＡＭ２２は、ＣＰＵ３０がプログラムを実行する際に各種データを一時的に格納するワークメモリや、回転処理等を施すために画像データを少なくとも１ページ分格納するページメモリとして機能する。

【００３７】

読取手段２３は、原稿画像を読み取って対応する画像データを取り込む機能を果たす。読取手段２３は、原稿を照射する光源と、原稿をその幅方向に１ライン分読み取るラインイメージセンサと、ライン単位の読取位置を原稿の長さ方向に移動させる移動手段と、原稿からの反射光をラインイメージセンサに導いて結像させるレンズやミラーから成る光学経路とを備えている。ラインイメージセンサはＣＣＤ（Charge Coupled Device）で構成される。ラインイメージセンサが出力するアナログ画像信号はＡ／Ｄ変換され、さらに誤差拡散処理等によって２値化され、各画素を深さ１ビットで表したデジタルの画像データとして出力される。

【００３８】

印刷手段２４は、画像データに対応する画像を電子写真プロセスによって記録紙上に形成して出力する機能を果たす。印刷手段２４は、記録紙の搬送装置と、感光体ドラムと、帯電装置と、レーザーユニットと、現像装置と、転写分離装置と、クリーニング装置と、定着装置とを有する、いわゆるレーザープリンタとして構成されている。ファクシミリ部２５は、ファクシミリとしての機能を果たす部分である。画像データをファクシミリに対応した圧縮方式で圧縮・伸張する機能や、ファクシミリ送受信のための各種通信手順を制御する機能を果たす。

【００３９】

表示操作部２６は、表面にタッチパネルを備えた液晶ディスプレイと各種の操作スイッチから構成され、ユーザーに各種の案内表示や状態表示を行なったり、ユーザーから各種の操作を受け付けたりする機能を有している。通信部２７は、電話回線や各種のネットワークと接続して通信する機能を果たす。

【００４０】

圧縮手段２８は画像データを圧縮する機能を果たし、伸張手段２９は、圧縮データを元の画像データに伸張する機能を果たす。圧縮は、先に説明したように、圧縮データの一部でも正しくないと伸張処理ができない圧縮方式で行なわれる。

【００４１】

画像データ制御部としてのＣＰＵ３０は、暗号キー抽出手段３１と、暗号化手段３２と、圧縮データ復元手段３３と、復元情報出力手段３４と、復元情報入力手段３５としての機能を果たす。暗号キー抽出手段３１は、圧縮手段２８によって画像データを圧縮して得た圧縮データの一部を暗号キーデータとして取り出す。暗号化手段３２は、圧縮データのうち暗号キーデータとして取り出された部分をこの暗号キーデータと異なるデータに置き換えて破壊することで、圧縮データを暗号化された暗号化データに変換する機能を果たす。圧縮データ復元手段３３は、暗号キーデータと暗号化データとを組み合わせて元の圧縮データに復元する機能を果たす。

【００４２】

復元情報出力手段３４は、暗号キー抽出手段３１が抽出した暗号キーデータと、この暗号キーデータに対応する暗号化データを特定するための特定情報とを関

連付けた復元情報を外部のユーザーに所定の形態で出力する機能を果たす。ここでは、指定されたアドレスに復元情報を電子メールで送信したり、復元情報を記録紙に印刷出力したりする。復元情報出力手段３４はこれらの動作を制御する機能を果たす。復元情報入力手段３５は、暗号キーデータとこれに関連付けされた特定情報とを含む復元情報を外部から入力する機能を果たす。入力は、表示操作部２６や通信部２７を通じて行なわれる。

【００４３】

補助記憶装置４０は、大容量の記憶装置である。ここではハードディスク装置を使用している。補助記憶装置４０は、圧縮データを暗号化手段３２によって暗号化して得た暗号化データを保存する暗号化データ保存手段としての機能を果たす。

【００４４】

不揮発性メモリ５０は、電源ＯＦＦ後も情報が記憶されるメモリであり、暗号キーデータを保存する暗号キー保存手段５１と、管理情報記憶手段５２としての機能を果たす。管理情報記憶手段５２は、同一の圧縮データから得た暗号キーデータと暗号化データとの対応付けを表した管理情報を記憶する。暗号化データは、ファイルとして補助記憶装置４０に記憶され、暗号化データとの対応付けを表す管理情報としてファイル名を用いるようになっている。具体的には、暗号キーデータとこれに対応する暗号化データが格納されているファイル名とを１組にして管理テーブルに格納することで、暗号キーデータと暗号化データとの対応付けが行なわれる。なお、暗号化データを格納したファイル名は、先に説明した特定情報としても使用される。

【００４５】

図３は、画像形成装置２０が画像データを圧縮し暗号化して保存する際の処理の流れを示している。まず、原稿を読み取って得た画像データ１０１を圧縮手段２８で圧縮して圧縮データ１０２を生成する（Ｓ１）。この際、原稿を１ページ毎に圧縮してページ毎の圧縮データを生成してもよいし、複数ページ分の画像データをまとめて圧縮し全体として１つの圧縮データを生成してもよい。

【００４６】

圧縮データ１０２の一部を暗号キーデータ１０３として取り出すとともに（Ｓ２）、データの一部が取り出された圧縮データ１０２のうち暗号キーデータが取り出された部分１０４のデータをゼロクリアして暗号化データ１０５に変換する（Ｓ３）。そして暗号化データ１０５をファイル化して補助記憶装置４０に保存するとともに（Ｓ４）、そのファイル名を管理情報として暗号キーデータ１０３と関連付けて管理テーブル１０６に登録する（Ｓ５）。管理テーブル１０６に登録された情報により、暗号キーデータとこれに対応する暗号化データの格納場所とが１対１に対応付けて管理保存される。

【００４７】

暗号化データ１０５は、暗号キーデータが取り出された部分１０４のデータがゼロクリアされて破壊されているので、元の画像データに伸張することはできない。したがって、補助記憶装置４０に保存してある暗号化データ１０５が不正な手段により取り出されて第三者の手に渡っても、そのデータだけでは元の画像データに伸張して復元することができず、高いセキュリティ性能を得ることができる。また、通常のユーザーは、画像形成装置２０の内部での暗号キーデータ１０３の管理方法や格納場所を知らないので、不正な手段を使っても暗号キーデータ１０３の入手が困難であり、高い機密性を確保することができる。

【００４８】

暗号キーデータ１０３として取り出すデータ量が多いほど、セキュリティレベルは高くなる。また圧縮データ１０２の先頭部分を暗号キーデータ１０３として取り出してその部分のデータをゼロクリアによって破壊するので、最初から一切の伸張処理ができなくなり、画像データの漏洩を強力に保護することができる。

【００４９】

画像データを保存する場合は、使用するメモリ量を低減するために、通常、圧縮処理が行なわれる。本発明では、この圧縮処理の結果として生成された圧縮データの性質を利用して暗号化しているので、暗号化に伴う追加処理が少なく、圧縮と暗号化とを効率よく実施することができる。

【００５０】

図４は、画像データを圧縮し暗号化して保存し、その復元情報を外部にネット

ワークを通じて送信する場合における処理の流れを示している。原稿を読み取って得た画像データ１０１を圧縮して圧縮データ１０２を生成し（Ｓ１１）、その一部を暗号キーデータ１０３として取り出す（Ｓ１２）。また暗号キーデータ１０３が取り出された部分１０４のデータをゼロクリアして圧縮データ１０２を暗号化データ１０５に変換し（Ｓ１３）、この暗号化データ１０５をファイル化して補助記憶装置４０に保存する（Ｓ１４）。このファイル名を、保存した暗号キーデータが取り出された部分１０４を特定するための特定情報とし、これと先の暗号キーデータ１０３とを関連付けた復元情報を外部の指定されたユーザーに送信する（Ｓ１５）。ここでは、通信部２７を用いて、電子メールまたはＦＴＰ等の処理でユーザーのパーソナルコンピュータ１１０にネットワークを通じて復元情報を送信している。

【００５１】

画像形成装置２０の補助記憶装置４０には暗号化データ１０５が保存されているが、これだけを第三者が不正に入手しても元の画像データに伸張することはできず、保存中の画像データに対するセキュリティ性が確保される。外部に送信する場合においても、暗号キーデータ１０３として取り出すデータ量が多いほど、セキュリティレベルが高くなる。

【００５２】

図５は、画像データを圧縮し暗号化して保存し、その復元情報を外部に印刷出力する場合における処理の流れを示している。原稿を読み取って得た画像データ１０１を圧縮して圧縮データ１０２を生成し（Ｓ２１）、その一部を暗号キーデータ１０３として取り出す（Ｓ２２）。また暗号キーデータ１０３が取り出された部分１０４のデータをゼロクリアして圧縮データ１０２を暗号化データ１０５に変換し（Ｓ２３）、この暗号化データ１０５をファイル化して補助記憶装置４０に保存する（Ｓ２４）。このファイル名と暗号キーデータ１０３とを関連付けた復元情報を印刷手段２４で記録紙１２０に印刷して出力する。復元情報の印刷された記録紙１２０には、ファイル名と暗号化データが印刷される。暗号化データは、データのダンプリストのようにして印刷される。すなわち、４ビット毎に０～９およびＡ～Ｆのいずれかの文字を用いて印刷される。

【００５３】

図６は、補助記憶装置４０に保存されている暗号化データを管理テーブル１０６に登録されている情報を用いて復元し伸張して、元の原稿画像データを出力する際のデータの流れを示している。ユーザーは、保存されているファイルを指定した印刷指示を表示操作部２６から入力する（Ｓ３１）。印刷指示を受けたＣＰＵ３０の圧縮データ復元手段３３は、指定されたファイルを補助記憶装置４０から読み出し、そのファイルに登録されている暗号化データ１０５をＲＡＭ２２の所定領域にセットする（Ｓ３２）。

【００５４】

次に、入力されたファイル名と対応付けられている暗号キーデータ１０３を管理テーブル１０６から取り出し（Ｓ３３）、これを暗号化データ１０５の中の暗号キーデータが取り出された部分１０４へコピーする（Ｓ３４）。これにより暗号化データ１０５は元の圧縮データ１０２に復元される。その後、圧縮データ１０２を伸張し（Ｓ３５）、元の原稿画像データを印刷手段２４で記録紙１３０に印刷して（Ｓ３６）出力する。

【００５５】

このように、画像形成装置２０の表示操作部２６から印刷指示を出す場合は、暗号キーデータ１０３を入力することなく画像を取り出して印刷することができ、ユーザーに画像形成装置２０内部での暗号化を意識させることなく通常の操作性を維持することができる。

【００５６】

図７は、補助記憶装置４０に保存されている暗号化データを、ネットワークを通じて外部に取り出し、ユーザーのパーソナルコンピュータ１１０で復元し伸張する場合におけるデータの流れを示している。ユーザーは保存されているファイルの送信指示をパーソナルコンピュータ１１０からネットワークを通じて画像形成装置２０に送信する（Ｓ４１）。送信指示を受けた画像形成装置２０の画像データ制御部（ＣＰＵ）３０は、指定されたファイルを補助記憶装置４０から読み出し、そのファイルに格納されている暗号化データ１０５をＲＡＭ2２の所定領域にセットする（Ｓ４２）。そして、この暗号化データ１０５を通信部２７に転

送し（Ｓ４３）、ネットワークを通じてユーザーのパーソナルコンピュータ１１０に送信する（Ｓ４４）。

【００５７】

画像形成装置２０からネットワークを通じて暗号化データ１０５を受け取ったユーザーのパーソナルコンピュータ１１０は、この暗号化データ１０５を内部のメモリに保存する（Ｓ４５）。そして、予め画像形成装置２０から受信していた暗号キーデータ１０３を暗号化データ１０５の中の暗号キーデータが取り出された部分１０４にコピーして圧縮データ１０２を復元し（Ｓ４６）、これを伸張する（Ｓ４７）。ユーザーのパーソナルコンピュータ１１０は、伸張した画像データあるいは復元した圧縮データ１０２を内部に保存することができる。

【００５８】

画像形成装置２０の補助記憶装置４０に保存されているデータは、様々な人がネットワークを通じて取り出し得るが、対応する復元情報を予め受け取っているユーザーだけが圧縮データ１０２に復元して元の画像データに伸張することができる。その結果、保存中の画像をネットワークを通じて遠隔から取り出す機能を画像形成装置２０が有する場合にも、保存中の画像は不正な第三者による閲覧から保護される。

【００５９】

図８は、補助記憶装置４０に保存されている暗号化データを、記録紙に印刷され出力された復元情報を用いて復元し伸張する場合におけるデータの流れを示している。ユーザーは、記録紙に印刷されている復元情報を参照して、印刷すべきファイルのファイル名と暗号キーデータを含む印刷指示を表示操作部２６から入力する（Ｓ５１）。印刷指示を受けた画像データ制御部（ＣＰＵ）３０は、指定されたファイルを補助記憶装置４０から読み出し、そのファイルに格納されている暗号化データ１０５をＲＡＭ２２の所定領域にセットする（Ｓ５２）。次に、表示操作部２６から入力された暗号キーデータ１０３を、暗号化データ１０５の中の暗号キーデータが取り出された部分１０４にコピーする（Ｓ５３）。これにより暗号化データ１０５は元の圧縮データ１０２に復元される。その後、圧縮データ１０２を伸張し（Ｓ５４）、元の原稿画像データを印刷手段２４で記録紙１

３０に印刷して（Ｓ５５）出力する。

【００６０】

次に本発明の第２の実施の形態について説明する。

第１の実施の形態では、圧縮データのうち暗号キーデータを取り出した部分をゼロクリアして破壊したが、第２の実施の形態では、暗号キーデータを取り出した部分を圧縮データから削除するようになっている。すなわち、図９に示すように、圧縮データ１５０を暗号キーデータの部分１５１とそれ以外の残り部分１５２とに分割する。残り部分１５２が暗号化データになる。復元は、暗号キーデータの部分１５１と残り部分１５２とを結合すればよい。このように暗号キーデータを取り出した部分を削除することで圧縮データを暗号化すれば、保存すべき暗号化データのデータ量が低減する。

【００６１】

次に本発明の第３の実施の形態としてのデータ秘密化装置およびデータ復元装置について説明する。図１０は、データ秘密化装置２００およびデータ復元装置２２０の構成をそれぞれ示している。データ秘密化装置２００には、圧縮データの一部でも正しくないと伸張処理ができない圧縮方式で圧縮された圧縮データが入力される。暗号キー抽出手段２０１は、図２に示した暗号キー抽出手段３１と同様に、圧縮データの一部を暗号キーデータとして取り出して出力する。暗号化手段２０２は、図２の暗号化手段３２と同様に、圧縮データのうち暗号キーデータとして取り出された部分をゼロクリア等して破壊することで暗号化した暗号化データを出力する。

【００６２】

データ復元装置２２０は、暗号キーデータと暗号化データとを入力し、これらを組み合わせて元の圧縮データに復元して出力する圧縮データ復元手段２２１を備えている。データ秘密化装置２００およびデータ復元装置２２０を用いることにより、圧縮された各種データを容易に暗号化したり、暗号化されたものを復号化したりすることが可能になる。

【００６３】

以上、本発明の各種実施形態を図面によって説明してきたが、具体的な構成は

実施の形態で例示したものに限られるものではなく、本発明の要旨を逸脱しない範囲における変更や追加があっても本発明に含まれる。たとえば、実施の形態では、暗号キーデータを取り出した部分をゼロクリアすることで圧縮データを暗号化したが、取り出した暗号キーデータと異なる値に変更し、その部分のデータが破壊されればよい。なお、元の暗号キーデータとまったく相違するようにデータの破壊を充分行なうことが望ましい。

【００６４】

また実施の形態では、圧縮データの先頭から所定範囲を暗号キーデータとして取り出したが、圧縮データの中の複数箇所から虫食いのように暗号キーデータを抽出してもよい。また抽出する場所をランダムに変化させ、抽出場所を示す情報についても別途暗号化するとよい。

【００６５】

さらに実施の形態では、暗号キーデータを管理テーブル１０６に記憶し、暗号化データを補助記憶装置４０に記憶したが、領域を分ければ、これらを同一の記憶媒体に記憶してもよい。なお、暗号キーデータと暗号化データを物理的に別の記憶媒体に分けて保存することにより、暗号化データの保存された補助記憶装置４０等が盗まれてデータの解析が行なわれた場合でも、復元することが不可能となり、高いセキュリティ性が確保される。

【００６６】

【発明の効果】

本発明に係るデータ秘密化装置、データ復元装置、画像データ保存装置および画像形成装置によれば、圧縮データの一部でも正しくないと伸張処理ができない圧縮方式で圧縮された圧縮データの一部を取り出して暗号キーデータとし、暗号キーデータとして取り出した部分の情報を破壊または領域を削除することで圧縮データを暗号化するので、簡単な処理で圧縮データを暗号化でき、特別なハードウェアの追加やＣＰＵに大きな負担をかけることなくデータを秘密化してセキュリティーを高めることができる。

【００６７】

特に画像データを保存する場合は、使用するメモリ量を低減するために、通常

、圧縮処理が行なわれるので、圧縮後の圧縮データが有する性質を利用して暗号化することで、暗号化に伴う追加処理が少なくなり、圧縮と暗号化とを効率よく実施することができる。

【図面の簡単な説明】

【図１】

本発明における暗号化および復号化における原理およびデータの流れを示す説明図である。

【図２】

本発明の第１の実施の形態に係る画像形成装置の構成を示すブロック図である。

【図３】

本発明の第１の実施の形態に係る画像形成装置が画像データを圧縮し暗号化して保存する際の処理の流れを示す説明図である。

【図４】

本発明の第１の実施の形態に係る画像形成装置が画像データを圧縮し暗号化して保存し、その復元情報を外部にネットワークを通じて送信する場合の流れを示す説明図である。

【図５】

本発明の第１の実施の形態に係る画像形成装置が画像データを圧縮し暗号化して保存し、その復元情報を外部に印刷出力する場合の流れを示す説明図である。

【図６】

本発明の第１の実施の形態に係る画像形成装置が補助記憶装置に保存されている暗号化データを管理テーブルに登録されている情報を用いて復元し伸張して元の画像データを出力する際のデータの流れを示す説明図である。

【図７】

本発明の第１の実施の形態に係る画像形成装置が補助記憶装置に保存されている暗号化データを、ネットワークを通じて外部に取り出し、ユーザーのパーソナルコンピュータで復元し伸張する場合におけるデータの流れを示す説明図である。

【図８】

本発明の第１の実施の形態に係る画像形成装置が補助記憶装置に保存されている暗号化データを印刷出力された復元情報を用いて復元し伸張する場合におけるデータの流れを示す説明図である。

【図９】

本発明の第２の実施の形態における暗号化・復号化の原理とデータの流れを示す説明図である。

【図１０】

本発明の第３の実施の形態にかかわるデータ秘密化装置およびデータ復元装置を示すブロック図である。

【符号の説明】

１０…画像データ

１１…圧縮データ

１１ａ…圧縮データの先頭から所定範囲の部分

１２…暗号キーデータ

１３…暗号化データ

２０…画像形成装置

２１…ＲＯＭ

２２…ＲＡＭ

２３…読取手段

２４…印刷手段

２５…ファクシミリ部

２６…表示操作部

２７…通信部

２８…圧縮手段

２９…伸張手段

３０…ＣＰＵ（画像データ制御部）

３１…暗号キー抽出手段

３２…暗号化手段

３３…圧縮データ復元手段

３４…復元情報出力手段

３５…復元情報入力手段

４０…補助記憶装置

５０…不揮発性メモリ

５１…暗号キー保存手段

５２…管理情報記憶手段

１０１…画像データ

１０２…圧縮データ

１０３…暗号キーデータ

１０４…暗号キーデータが取り出された部分

１０５…暗号化データ

１０６…管理テーブル

１１０…ユーザーのパーソナルコンピュータ

１２０…復元情報の印刷された記録紙

１３０…元の原稿画像データの印刷された記録紙

１５０…圧縮データ

１５１…暗号キーデータの部分

１５２…残り部分

２００…データ秘密化装置

２０１…暗号キー抽出手段

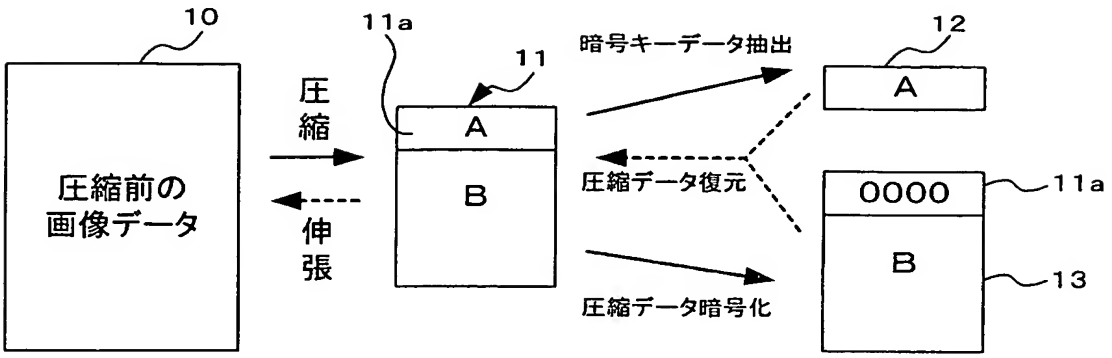
２０２…暗号化手段

２２０…データ復元装置

２２１…圧縮データ復元手段

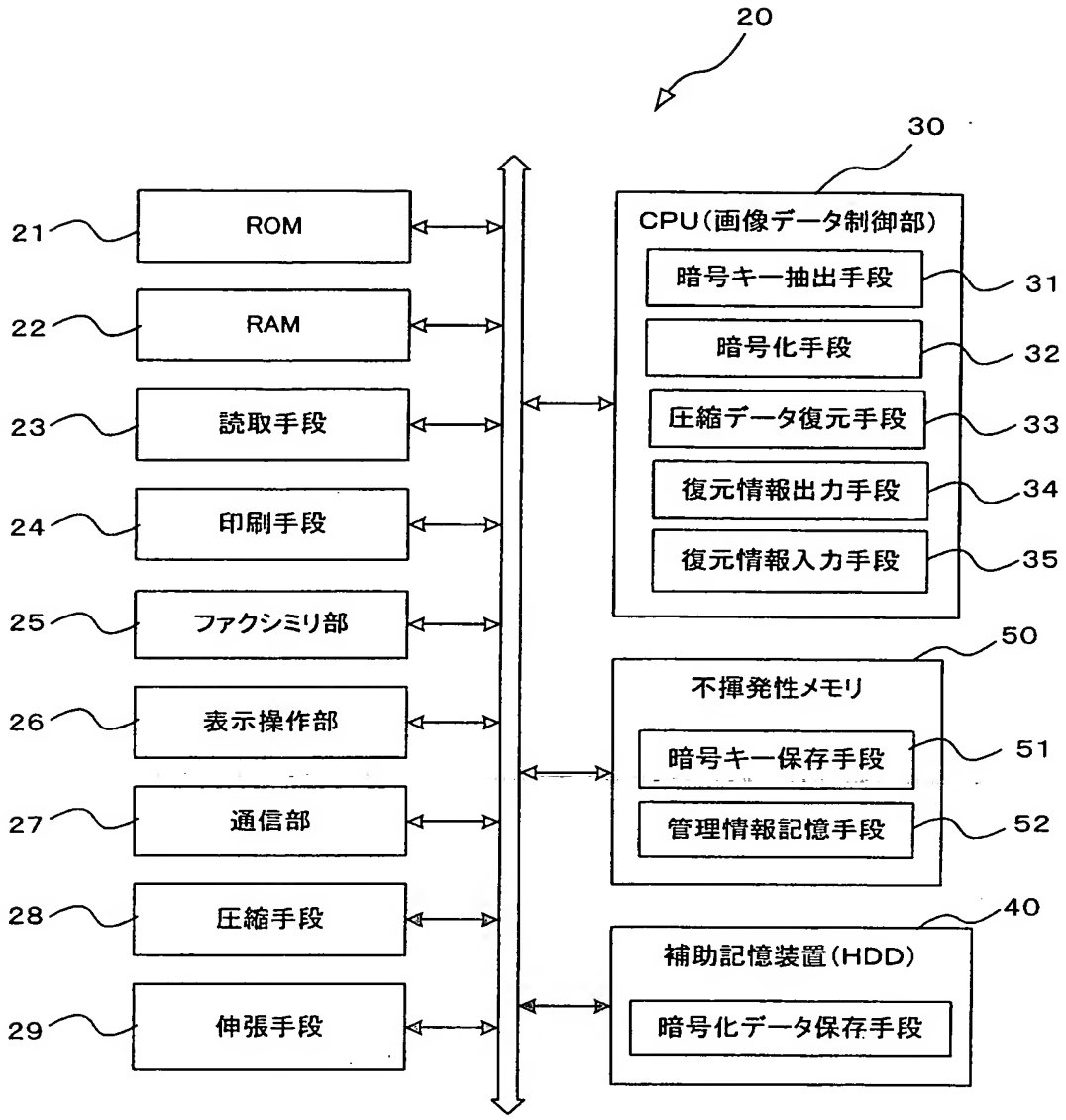
【書類名】図面

【図１】

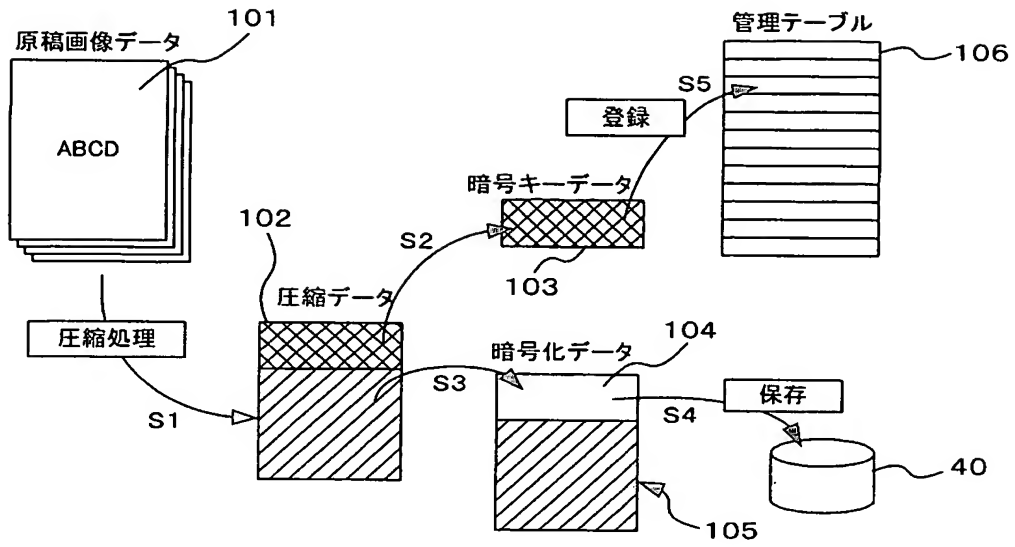


11 ・・・・圧縮データ
11a・・・・ゼロクリアによりデータ破壊した領域
12 ・・・・暗号キーデータ
13 ・・・・暗号化データ

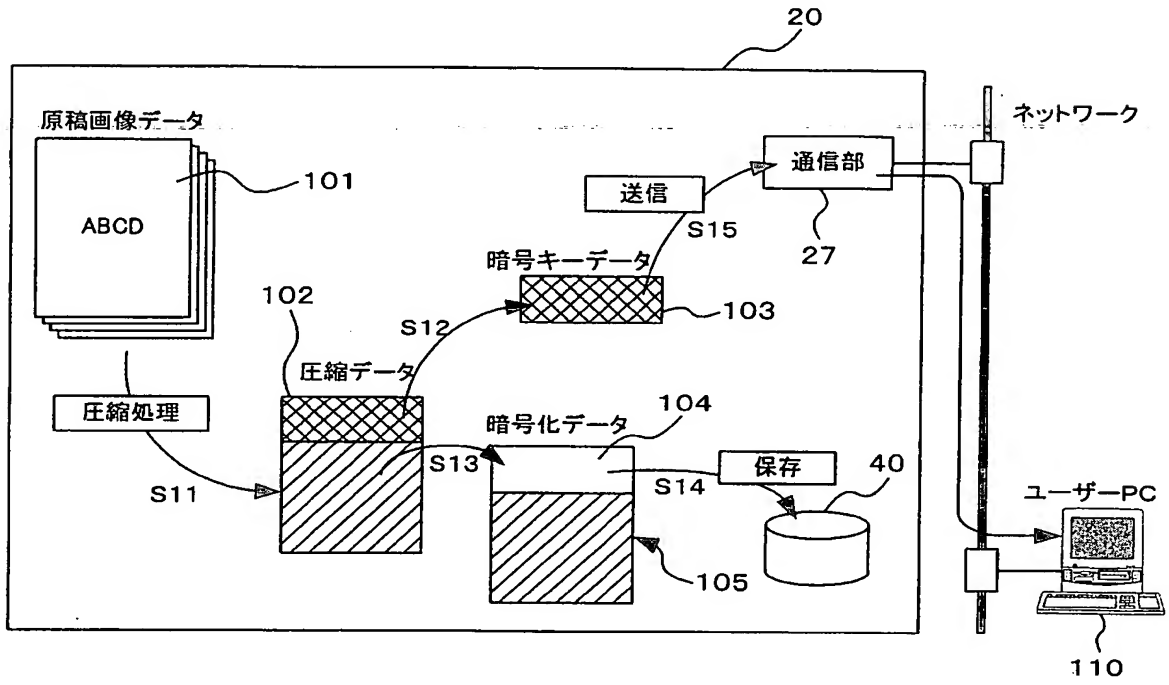
【図２】


20
30
CPU(画像データ制御部)
暗号キー抽出手段
31
暗号化手段
32
圧縮データ復元手段
33
復元情報出力手段
34
復元情報入力手段
35
21
ROM
22
RAM
23
読取手段
24
印刷手段
25
ファクシミリ部
26
表示操作部
27
通信部
28
圧縮手段
29
伸張手段
50
不揮発性メモリ
暗号キー保存手段
51
管理情報記憶手段
52
40
補助記憶装置(HDD)
暗号化データ保存手段

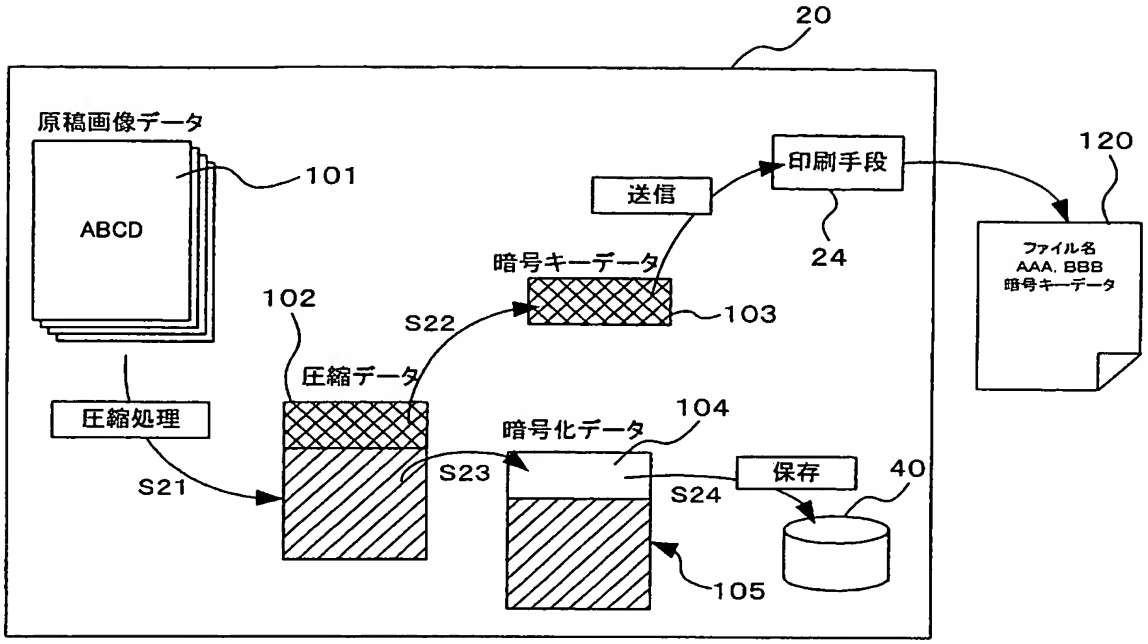
【図３】


原稿画像データ
101
ABCD
圧縮処理
102
圧縮データ
S1
S2
暗号キーデータ
103
管理テーブル
106
S5
登録
S3
暗号化データ
104
S4
保存
40
105

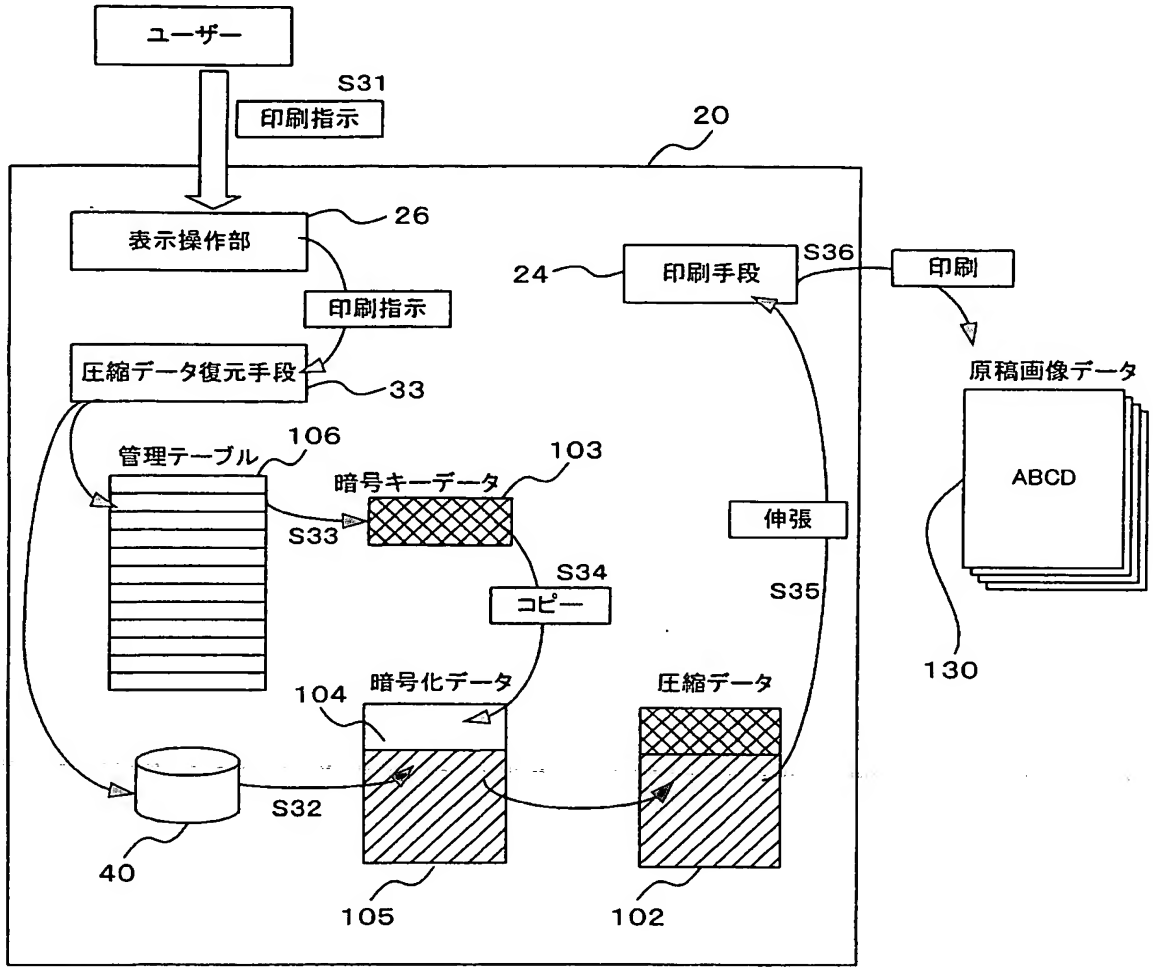
【図４】


20
原稿画像データ
ABCD
101
圧縮処理
102
圧縮データ
S11
S12
暗号キーデータ
103
送信
S15
通信部
27
ネットワーク
S13
暗号化データ
104
S14
保存
40
105
ユーザーPC
110

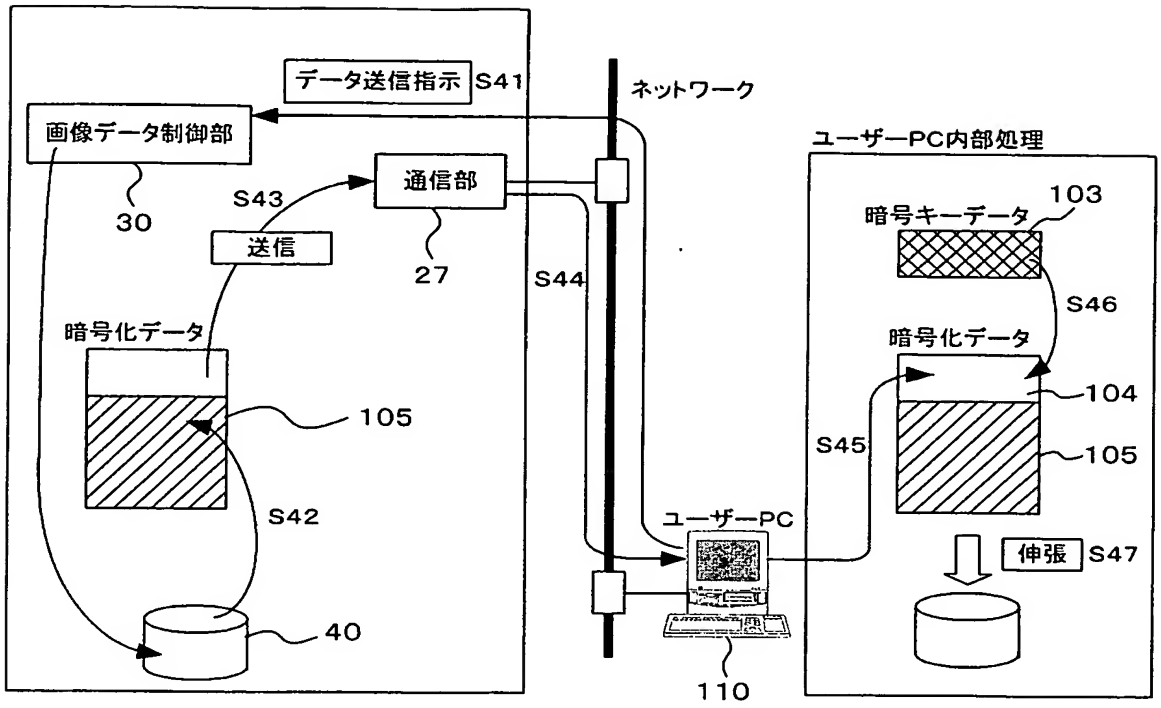
【図５】


20
原稿画像データ
101
ABCD
圧縮処理
S21
102
圧縮データ
S22
暗号キーデータ
103
送信
印刷手段
24
120
ファイル名
AAA, BBB
暗号キーデータ
104
暗号化データ
S23
S24
保存
40
105

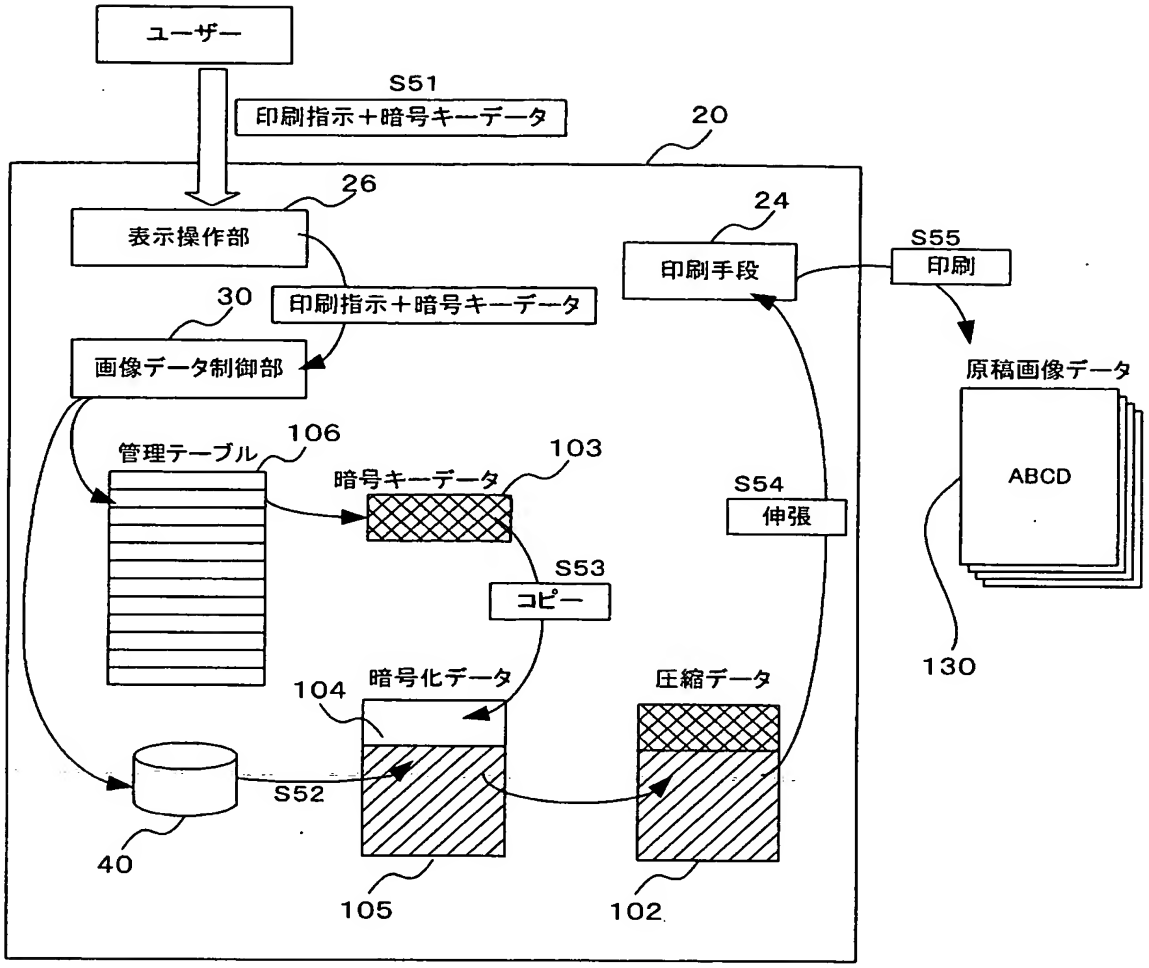
【図６】


ユーザー
S31
印刷指示
20
表示操作部
26
印刷指示
圧縮データ復元手段
33
24
印刷手段
S36
印刷
原稿画像データ
ABCD
130
管理テーブル
106
暗号キーデータ
103
S33
伸張
S34
コピー
S35
暗号化データ
104
圧縮データ
S32
40
105
102

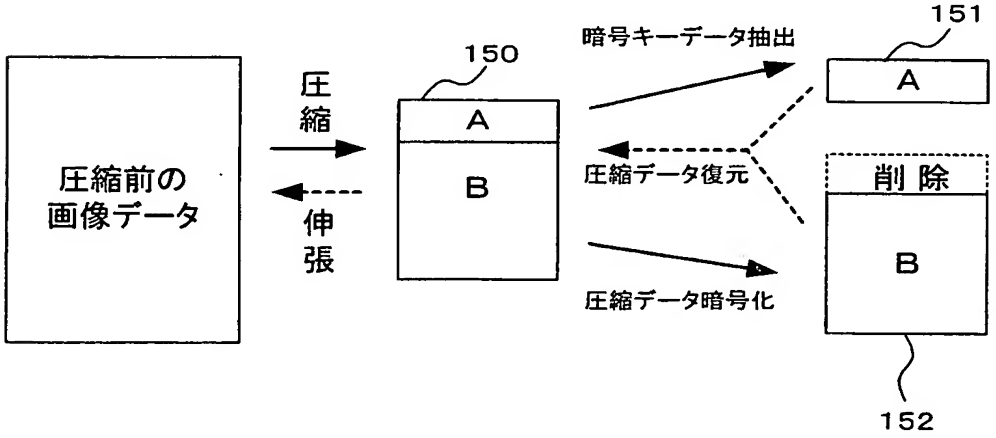
【図７】


データ送信指示
S41
ネットワーク
画像データ制御部
30
通信部
27
S43
送信
S44
暗号化データ
105
S42
40
ユーザーPC
110
ユーザーPC内部処理
暗号キーデータ
103
S46
暗号化データ
104
S45
105
伸張
S47

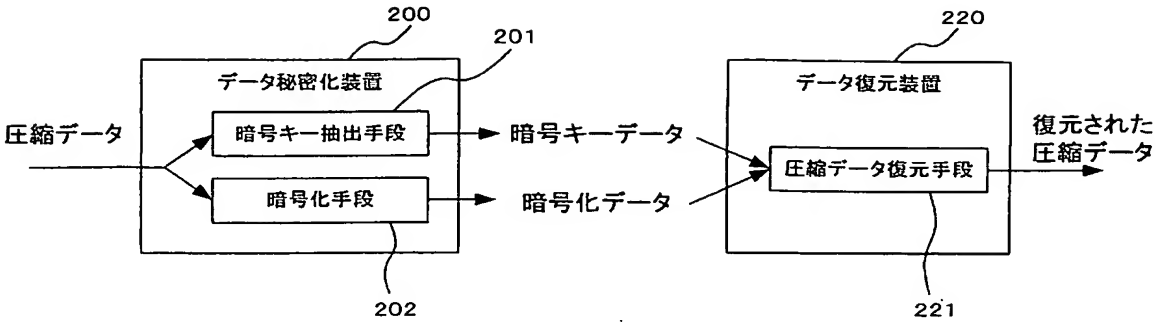
【図８】


ユーザー
S51
印刷指示＋暗号キーデータ
20
26
表示操作部
24
印刷手段
S55
印刷
30
印刷指示＋暗号キーデータ
画像データ制御部
原稿画像データ
管理テーブル
106
暗号キーデータ
103
S54
伸張
ABCD
S53
コピー
130
暗号化データ
104
圧縮データ
S52
40
105
102

【図９】


圧縮前の
画像データ
圧
縮
伸
張
150
A
B
暗号キーデータ抽出
151
A
圧縮データ復元
削 除
B
圧縮データ暗号化
152

【図１０】


200
201
データ秘密化装置
圧縮データ
暗号キー抽出手段
暗号化手段
暗号キーデータ
暗号化データ
202
220
データ復元装置
圧縮データ復元手段
復元された
圧縮データ
221

【書類名】要約書

【要約】

【課題】特別なハードウェアの追加やＣＰＵに大きな負担をかけることなく、画像データを高速に暗号化・復号化する。

【解決手段】圧縮データ１１の一部でも正しくないと伸張処理ができない圧縮方式で画像データ１０を圧縮し、圧縮データ１１の一部を暗号キーデータ１２として取り出し、圧縮データ１１のうち暗号キーデータ１２を取り出した部分をゼロクリアして暗号化データ１３に変換する。暗号化データ１３は先頭部分のデータが破壊されているので、復元できない。また圧縮データの性質を利用して復元不能にするので、簡単な処理で暗号化・復号化ができる。

【選択図】図１

認定・付加情報

特許出願の番号	特願２００３－１８２２２２
受付番号	５０３０１０６５１７４
書類名	特許願
担当官	第一担当上席　　００９０
作成日	平成１５年　６月２７日

＜認定情報・付加情報＞

【提出日】　平成15年 6月26日

次頁無

特願２００３－１８２２２２

出　願　人　履　歴　情　報

識別番号　［３０３０００３７２］

１．変更年月日　２００２年１２月２０日
［変更理由］　新規登録
住　所　東京都新宿区西新宿１丁目２６番２号
氏　名　コニカビジネステクノロジーズ株式会社

２．変更年月日　２００３年１０月　１日
［変更理由］　名称変更
住所変更
住　所　東京都千代田区丸の内一丁目６番１号
氏　名　コニカミノルタビジネステクノロジーズ株式会社